RFINITY

## Reduced Trust in Transaction Technologies Results in Reduced Profits

Over the last 3 years, hundreds-of-millions of individuals around the world have had their personal financial information compromised and misused. Billions have read about the subsequent cases of identity theft, fraudulent transactions, and associated criminal activities enabled by static account numbers. The net-effect of the unauthorized use of credit card and personal identification numbers is a significant loss of opportunities for merchants and banks. In a July 2008 report published by Deloitte Consulting, one third of fraud victims surveyed stated that they had reduced or terminated their relationship with the bank or card issuer as a result of fraudulent use of their account information.[i]

The increase in the costs associated with fraud recovery programs and fraud-prevention regulatory requirements such as the Payment Card Industry Data Security Standard (PCI-DSS), combined with the decrease in account usage, results in significant reductions in card issuer profit margins. Organized criminal organizations are constantly developing increasingly sophisticated schemes to profit from the weaknesses in the current payment card system architecture and implementation.[ii]

The net effect of the increased fraud, reduced usage and increasing criminal attention is a real threat to the very viability of the payment card industry. Without a significant improvement in the technologies that are used in the payment system, the only group that will increase their profits will be the criminals.

## RFINITY – Security and Convenience Combined on a New Platform

At a US government research laboratory, a group of infrastructure security experts were testing potential solutions to the threats facing the current payment system. In analyzing the problem, the root cause of the existing threat and vulnerability landscape was determined to be the use of static numbers and rudimentary encryption systems that relied on decades-old technologies.

The solutions were obvious, protect the transactions with modern cryptography (AES, ECC) and a reliable one-time-use encoding system – the risks could be mitigated. But this technology would require that users have a personal and portable power source to enable patented security technology developed by RFinity. The near-ubiquitous deployment of mobile phones now has created a unique opportunity to take the generational leap forward to exponentially increase the security of identity and transaction technologies.

RFinity technology allows the billions of people who carry a reliable energy source a unique opportunity to deploy the next-generation in identity and transaction technology. The mobile phones that over 3 billion people around the world use on a daily basis are now capable of high-power encryption, generating one-time-use codes, managing complex trust relationships, and actively protecting sensitive information from malicious attacks.

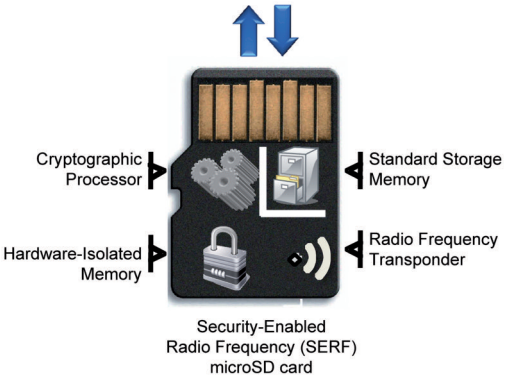
The RFinity platform architecture allows approved partners to develop their own custom implementation on top of US-government developed security technology designed to meet the highest standards of integrity. The components of the RFinity platform are:

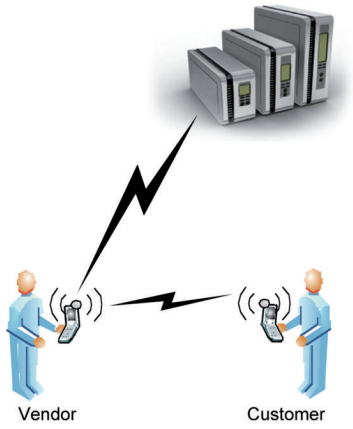
- **Security-enabled microSD card:** designed to fit into existing mobile phones and already-deployed transaction terminals; ensures the integrity of transactions by separating the user's transaction engine from vulnerable handsets and computing systems; all microSD cards are capable of being a token as well as a terminal – allowing for new transaction opportunities

- **Peer-to-peer distributed transaction handling:** implemented in a design that eliminates the hub-and-spoke vulnerabilities of existing systems; without a single point to target, criminals' probability of success in predicting, cloning or replaying transactions is significantly reduced

- **One-time-use payment codes:** each time an RFinity user identifies themselves or makes a payment the transaction is identified with a uniquely-random code; migration to the RFinity platform eliminates the need to implement and audit for PCI-DSS compliance resulting in significant operational cost savings

- **Automated Clearing House (ACH) interface:** RFinity's platform is designed to integrate directly with the ACH network, providing a low-cost and reliable transaction conduit




## The Future of Identification and Transactions is RFinity

With the RFinity microSD card installed in a supported handset, an individual now has a secure means of presenting payment to others as well as having the capability to receive payments as well. RFinity users no longer have to worry about stolen credit card numbers, as each time they use the RFinity platform their transaction is encoded within a unique, one-time-use identifier. RFinity issuers will no longer have to forecast what their fraud losses will be. Merchants accepting RFinity will no longer have to budget for PCI-DSS compliance and audit. All of this is accomplished using an amazing new platform that combines the security of high-integrity encryption with the convenience of near-field communications. Point two RFinity-enabled mobile phones at each other, the seller requests payment, the buyer confirms the transaction and within seconds all parties know that they have conducted a transaction they can trust.

RFINITY

901 Pier View Drive, Suite 207
Idaho Falls, Idaho 83404
USA
contact@rfinity.net
**www.rfinity.net**
+1 (208) 346-7330

[i] Building Consumer Trust in Retail Payments
http://www.deloitte.com/dtt/cda/doc/content/us_fsi_Bank_ConsumerTrustPayments_July08.pdf

[ii] Technical Report: Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones
http://honeyblog.org/archives/8-Technical-Report-Learning-More-About-the-Underground-Economy-A-Case-Study-of-Keyloggers-and-Dropzones.html